

A circular portrait of Kandyce Young, a Black woman with long dark hair, wearing a light blue pinstriped blazer over a white lace top. The portrait is set against a dark teal background with colorful abstract shapes (green, blue, orange, purple) around it.

# Kandyce Young

Senior Technical Product Manager  
PCI Security Standards Council

2025  
EUROPE  
COMMUNITY  
MEETING

# Securing Data, Strengthening Environments:

The Past, Present, and Future

# Data and Environment Security

PCI  
DSS

PCI Token  
Service  
Providers  
(TSP)

PCI  
3DS Core

A close-up photograph of a black car side mirror. The mirror's reflection shows the text 'PCI DSSv1.1' in a bold, teal, sans-serif font, with 'The Past' in a smaller, teal, italicized serif font below it. The background of the reflection is white. The car's body is dark, and a large orange circle is partially visible in the top right corner of the frame. A purple circle is partially visible in the bottom left corner.

**PCI DSSv1.1**  
*The Past*



**2006:  
Threat Landscape**



**2006:  
Threat Landscape**



**Payment Card Industry (PCI)  
Data Security Standard**

**Version 1.1**  
Release: September, 2006

# PCI DSS v1.1

Published in Sept 2006

# PCI DSS v1.1 Requirements

Security Standard (DSS)  
related groups, which are

sensitive authentication data;  
each data element must be  
different types of requirements

is stored, processed, or  
requirements do not apply.

Protection required	PCI DSS Req. 3.4
YES	YES
NO	NO
NO	NO
NO	NO
N/A	N/A
N/A	N/A
N/A	N/A

any protection must be consistent  
Additionally, other legislation (for  
data security) may require specific  
related personal data is being  
are not stored, processed, or  
even if encrypted).

Components are defined as any  
to the cardholder data  
that possesses cardholder data  
isolates systems that store,  
the scope of the cardholder data  
switches, routers, wireless  
types include but are not limited  
protocol (NTP), and domain  
connections, including internal and

## Build and Maintain a Secure Network

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**  
Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

- 1.1 Establish firewall configuration standards that include the following:
  - 1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration
  - 1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks
  - 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
  - 1.1.4 Description of groups, roles, and responsibilities for logical management of network components
  - 1.1.5 Documented list of services and ports necessary for business
  - 1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)
  - 1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features
  - 1.1.8 Quarterly review of firewall and router rule sets
  - 1.1.9 Configuration standards for routers.
- 1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.
- 1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:
  - 1.3.1 Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)
  - 1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ
  - 1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)
  - 1.3.4 Placing the database in an internal network zone, segregated from the DMZ
  - 1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment
  - 1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration



# PCI DSS v4.0.1

*The Present*



# Current Threat Landscape



# Current Threat Landscape

# Recent Publications

E-commerce Requirements Guidance

Integrating AI in PCI Assessments

Vulnerability Management Infographic

Authentication Guidance

Authentication Guidance Summary

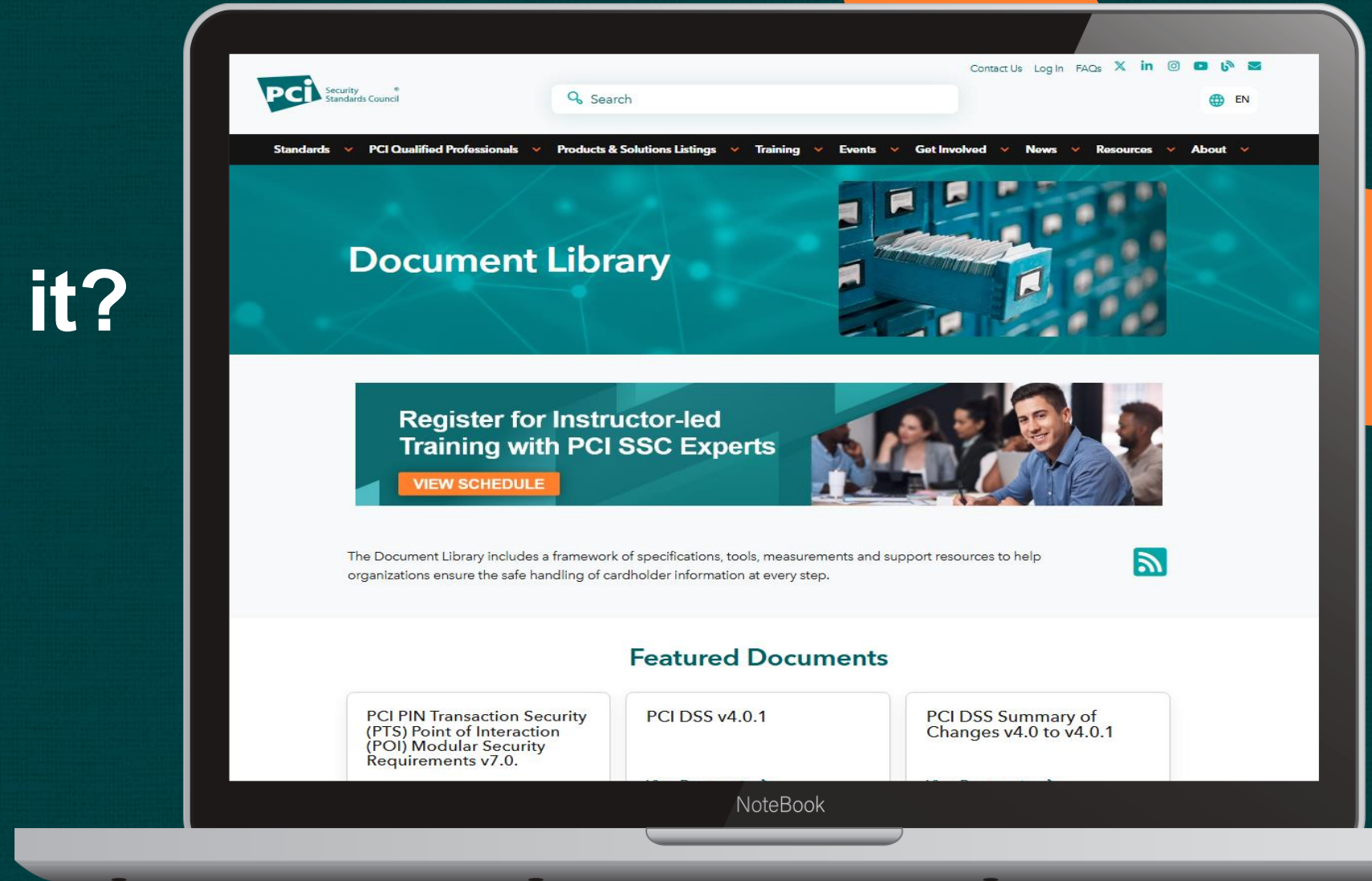
Cryptography Guidance

FAQs

AI Principles

Translations

# Where to find it?





# PCI DSS Evolved

## *The Future*

# PCI DSS Evolved

## *The Future*

Cloud  
Tokenization  
Services ↑ 20%

32% of all  
e-com payments  
are tokenized

# PCI DSS Evolved

## *The Future*


Cloud  
Tokenization  
Services ↑ 20%

32% of all  
e-com payments  
are tokenized



## PCI SSC's Mission Isn't Changing:


*Our role is to enhance global payment account data security by developing standards and supporting services that drive **education, awareness, and effective implementation** by stakeholders.*








## PCI SSC's Mission Isn't Changing:

*Our role is to enhance global payment account data security by developing standards and supporting services that drive **education, awareness, and effective implementation** by stakeholders.*



# *PCI DSS Evolution: Why Now?*

-  **Security and risk responsibility moving upstream**
-  **Opportunity to build in risk management considerations**
-  **Maintaining industry baselines remains essential**
-  **PCI community uniquely positioned to build future frameworks**

# *PCI DSS Evolution: Approach*



**1.**

Respond to industry demand to address evolving payments landscape

**2.**

Evolve to support risk-based security controls for payment environments with no/limited PAN

**3.**

Ensure that security implementation costs align to security benefits

# *PCI DSS Evolution: Approach*



**1.**

Respond to industry demand to address evolving payments landscape

**2.**

Evolve to support risk-based security controls for payment environments with no/limited PAN

**3.**

Ensure that security implementation costs align to security benefits

# PCI DSS Evolution: Goals



Establish environmental security structure not solely based on PAN



Provide flexibility to apply security rigor based on risk



Distinguish between complex and simple environments



Define clear scope impact for use of PCI SSC validated solutions



Optimize and modernize validation documents

# Global Stakeholder Collaboration Opportunities

1. What's the best way to reach these goals?

2. What's a realistic timeframe?

3. What are the industry needs to support preparedness?



Find the shapes.

 roll	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 stack	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 slide	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>

Level 39





Not quite, try again...



Find the shapes.

 roll	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 stack	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 slide	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>



Level 39





Not quite, try again...

“all”



Find the shapes.

 roll	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 stack	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
 slide	 <input type="checkbox"/>	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>



Level 39





Find the shapes.

<b>roll</b> 	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>
<b>stack</b> 	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input type="checkbox"/>	 <input type="checkbox"/>
<b>slide</b> 	 <input type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>	 <input checked="" type="checkbox"/>



Level 39



# PCI SSC Stakeholders



# PCI SSC Stakeholders



# Now What?

Visit the PCI SSC Booth

Share Bold Ideas

Bookmark [www.PCISSC.org](http://www.PCISSC.org)

Connect with Others



# 2025 EUROPE COMMUNITY MEETING